



Oktatás, kutatás,
gyógyítás: 250 éve az
egészség szolgálatában

Adatvédelmi incidensek

Csaba László

2020. december 28.



Mi az adatvédelmi incidens?

...a **biztonság** olyan **sérülése**, amely a továbbított, tárolt vagy más módon kezelt **személyes adatok** véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;



GDPR 4. cikk 12.

Adatvédelmi incidens besorolása

1) Bizalmassági incidens

- ➔ személyes adatok véletlen vagy felhatalmazás nélküli közlése vagy az ezekhez való hozzáférés.

2) Sértetlenséggel kapcsolatos incidens

- ➔ személyes adatok véletlen vagy jogtalan megváltoztatása.

3) Rendelkezésre állással kapcsolatos incidens

- ➔ személyes adatok véletlen vagy jogtalan megsemmisítése vagy ezek elvesztése.



Adatvédelmi incidens típusai példák

1) Titoktartási incidens

- Személyes adatok véletlen vagy felhatalmazás nélküli közlése vagy a személyes adatokhoz való hozzáférés.
- Ezek alapján egy szélesebb személyi kör férhet az adathoz, mint amiről az érintettnek tudomása van.
- Ilyen esetben a személyes adat bizalmas jellege sérül.

➤ *Például*

Az Adatkezelő az érintett hozzájárulása vagy jogszabály felhatalmazása nélkül lemásolta a betegek adatait és azt továbbította.



Adatvédelmi incidens típusai példák

2) Hozzáférhetőséggel kapcsolatos incidens

- A személyes adatok véletlen vagy jogosulatlan megsemmisítése vagy ezek elvesztése.
- Ilyen esetben a rendelkezésre állás elve sérül.

→ *Például*

Az Adatkezelő számítógépét ellopták, amely tartalmazta az egészségügyi dokumentációt, így a betegek nevét, címét és telefonszámát, illetve egészségügyi adataikat.

Az adatokról nem készült biztonsági másolat és az adatok nem voltak titkosítva, így az Adatkezelőnek nem áll rendelkezésére az egészségügyi dokumentáció.



3. Sértetlenséggel kapcsolatos incidens

- ↪ A személyes adatok véletlen vagy jogosulatlan megváltoztatása.
- ↪ Ez esetben az integritás, mint adatkezelési alapelv sérül.

↪ *Például*

Az Adatkezelő a belső elektronikus nyilvántartásban az egyik beteg nevét véletlenül az összes többi beteg neveként is beállította, törölve ezzel a korábbi neveket.



Adatvédelmi incidens vagy információbiztonsági?



ÉS / VAGY



Adatvédelmi incidens vagy információbiztonsági?

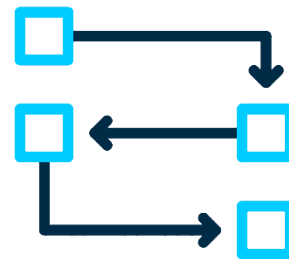


adatvedelem@semmelweis-univ.hu

infobiztonsag@semmelweis.hu

Az adatvédelmi incidens kezelésének folyamata

- 1) Incidens beazonosítása
- 2) Kockázat felmérése
- 3) Hatósági bejelentés
- 4) Szükség esetén érintettek tájékoztatása
- 5) Korrekciós intézkedések



- *A következő részben megnézzük mi a teendő, ha adatvédelmi incidens bekövetkezett.*





*Oktatás, kutatás,
gyógyítás: 250 éve az
egészség szolgálatában*

2. rész

Az adatvédelmi incidens esetén a **teendők**

Csaba László



2020. december 28.

Mi a teendő, ha adatvédelmi incidens következett be?

- 1) Felesleges pánikba esni.
- 2) Mindent el kell követni, hogy csökkentsük a további veszteséget, megelőzzük a további károkat.
- 3) Értékelni kell, hogy mekkora kockázattal jár az érintettekre nézve az incidens.
- 4) Értesítési kötelezettség teljesítése



Az adatvédelmi incidens kezelése

1. Az **adatkezelő nyilvántartja** az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.
2. Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, **legkésőbb 72 órával azután**, hogy az adatvédelmi incidens a tudomására jutott, **bejelenti a felügyeleti hatóságnak**, **kivéve**, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.
3. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül **tájékoztatja az érintettet** az adatvédelmi incidensről.



Az adatvédelmi incidens bejelentése (1)

Az **adatkezelő nyilvántartja** az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.



GDPR 33. cikk (5) bekezdés.

Az adatvédelmi incidens bejelentése (2)

Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb **72 órával** azután, hogy az adatvédelmi incidens a **tudomására jutott**, **bejelenti** a **felügyeleti hatóságnak**, **kivéve**, ha az adatvédelmi incidens valószínűsíthetően **nem jár kockázattal** a természetes személyek jogaira és szabadságaira nézve.



GDPR 33. cikk (1) bekezdés.

Az adatvédelmi incidens jelentése (3)

Ha az adatvédelmi incidens valószínűsíthetően **magas kockázattal jár** a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül **tájékoztatja az érintettet** az adatvédelmi incidensről.



GDPR 34. cikk (2) bekezdés.

Mit jelent a magas kockázat?

... valószínűsíthetően **magas kockázattal** jár a természetes személyek jogaira és szabadságaira nézve

- ☐ Nagy mennyiségű személyes adat kezelése történik
- ☐ Érintettek nagy száma
- ☐ Hátrányos megkülönböztetés történhet
- ☐ Ha kiszolgáltatók személyes adatait kezelik (pl. gyermek)
- ☐ Az érintettek nem rendelkezhetnek saját személyes adataik felett
- ☐ A személyazonossággal való visszaélés
- ☐ A profilalkotás
- ☐ Viselkedés vagy mozgás követése történik
- ☐ Különleges adatokat kezelnek
- ☐ A jó hírnév sérelme megvalósul
- ☐ Az incidens fizikai, vagyoni vagy nem vagyoni károkhoz vezet



GDPR Preambulum (75)



Érintettek értesítése

1. Ha az adatvédelmi incidens valószínűsíthetően **magas kockázattal** jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.
2. **Indokolatlan késedelem nélkül**



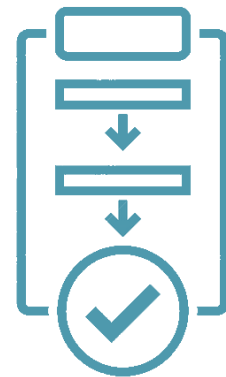
Milyen tartalmú tájékoztatást kell nyújtani az érintetteknek?



1. **Ismertetni kell** az adatvédelmi incidens jellegét.
2. **Közölni kell** az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit.
3. **Ismertetni kell** az adatvédelmi incidensből eredő, valószínűsíthető következményeket.
4. **Ismertetni kell** az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.
5. **Lényeges**, hogy az adatkezelő arról is tájékoztassa az érintettet, hogy hogyan tud védekezni a lehetséges hátrányos következményekkel szemben.

Az incidens kezelésének belső eljárásrendjéről

1. **El kell kerülni** egy széthúzó, nem egységes reagálást az incidensre.
2. Történjen meg az **incidens** bekövetkeztének a **bizonyítása**, megerősítése, ...
3. ... gyors körülhatárolása, megfékezése.
4. Az incidensben érintett személyes adatok körének **minimalizálása** valósuljon meg.
5. Az adatkezelési műveletekben fellépő zavar **elhárítása**.
6. **Az incidenssel kapcsolatos** bizonyítékok megfelelő azonosítása és rögzítése történjen.
7. **Megfelelő ajánlások** és biztonsági lépések megfogalmazására kerüljön sor.



Korrektíós intézkedések

1. Okozott **hátrányok** felszámolása.
2. **Érintettek** értesítése – aktivizálása.
3. Hibajavítás.
4. Gyökér-**ok** felkutatása, felszámolása.
5. Jövőben hasonló eset **ne fordulhasson elő**.
6. Gyakran szervezési **intézkedés**, kontroll bevezetése.
7. **Oktatás**: bekövetkezési valószínűség csökkentése.



Felmerülő kérdések

1. Az informatikai incidens azonos az adatvédelmi incidenssel?

➔ Nem. A fő különbség, hogy az adatvédelmi incidens az „érintettek jogaira vagy szabadságaira„ jelentett kockázatot nézi.

2. Incidens-e, ha e-mailben kapunk egy átveréses megkeresést? (Nigériai örökség, stb).

➔ Nem, mert nem társul hozzá cselekmény.

3. Incidens, ha az e-mailben az szerepel, hogy eltüntették a fájlokat és visszaállítják később?

➔ Igen.



➤ *A harmadik részben a példák következnek*





*Oktatás, kutatás,
gyógyítás: 250 éve az
egészség szolgálatában*

3. rész

Adatvédelmi incidensekre példák

Csaba László



2020. december 28.

Példák az adatvédelmi incidensre (1)

- ☐ Előre nem látható **károsodás** éri az eszközeinket, pl. tűz- vagy vízkár.
- ☐ **Elveszítjük** vagy **ellopják** a laptopot, pendrive-ot, amin személyes adatokat tárolunk.
- ☐ **Rossz helyre** küldjük az e-mailt, amely személyes adatokat tartalmaz.
- ☐ **Nyilvánosságra hozunk** egy fényképet, amelyet nem lett volna szabad.
- ☐ **Megtévesztéssel** vagy más úton információt szereznek az adatokról illetéktelenek.
- ☐ **Átadjuk** a jelszavainkat valakinek, aki jogosulatlanul hozzáfér a személyes adatokhoz.
- ☐ Egy kibertámadás következtében orvosi felvételek órákon át **nem elérhetőek** egy kórházban.



Példák az adatvédelmi incidensre (2)

- ☐ Személyes adatok **nagy nyilvánosság** előtti jogellenes közzététele - ilyen például, amikor a levelezőlistában az összes címzett látja a többi email címet is.
- ☐ Személyes **adatok jogellenes megismerése** illetéktelen hozzáféréssel - mint például egy hackertámadás vagy vírustámadás.
- ☐ **Jogosulatlan fényképfelvétel** készítés harmadik személy által különböző nem biztonságosan tárolt, ügyféladatokat tartalmazó dokumentumokról.
- ☐ Az adatkezelő nem biztosította a **leiratkozás** lehetőségét az általa kiküldött hírlevélről.
- ☐ Személyes adatok feletti **rendelkezés elvesztése** az adatok zsarolóvírus általi titkosításával.
- ☐ **Személyiséglopás** az érintett email címe feletti rendelkezés átvételével és nevében illetéktelen üzenetküldéssel.
- ☐ Egy személy felhívja a bankot és bejelenti, hogy valaki **más** havi banki kimutatását kapta meg.



Példa (minta)

Egy kórházi dolgozó úgy dönt, hogy lemásolja a betegek adatait egy CD-re és közzéteszi őket az interneten.

↘ A kórház néhány nappal később felfedezi a történeteket.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
?	?	?



Példa (minta)

Egy kórházi dolgozó úgy dönt, hogy lemásolja a betegek adatait egy CD-re és közzéteszi őket az interneten.

↪ A kórház néhány nappal később felfedezi a történeteket.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	IGEN	IGEN
		



Példa (1)

Az Egyik Klinika alkalmazottainak adatai nyilvánosságra kerültek.

➤ Az adatok között szerepel az alkalmazottak lakcíme, családi állapota, havi bevétele és minden alkalmazott egészségügyi kiadása.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	IGEN	IGEN
		

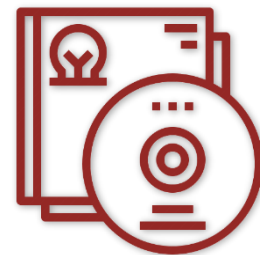


Példa (2)

A bérszámfejtést tartalmazó adatbázist biztonsági okokból lementik egy DVD-re.

- A DVD-t zárt borítékban küldik el az egyik épületből a másikba, amely közben a boríték eltűnik.
- Két héttel később a boríték bontatlanul előkerül a másik épületben, ugyanis két hasonló nevű munkatárs közül a nem megfelelőnek adták át a DVD-t.
- A munkatárs azonban szabadságon volt, így nem tudta a jó címzettnek odaadni.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	NEM	NEM
		

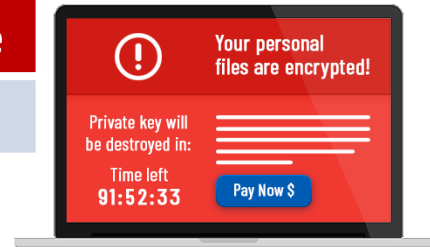


Példa (3)

A központi számítógépet zsarolóvírus támadás érte.

- ✎ Az informatika segítségével megállapításra került, hogy kifelé irányuló forgalom nem történt a gépről.
- ✎ A zsaroló vírus csak a fájlokat titkosította, nem másolta le azokat.
- ✎ Az érintett személyes adatok a munkavállalók és ügyfelek személyes adatai.
- ✎ Minden nap végén külső merevlemezre biztonsági másolat készült.
- ✎ A biztonsági másolatból 4 órával a fertőzés megszüntetését követően helyreállították a személyes adatokat.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	NEM	NEM
		



Példa (4)

A helyi Egyik Szakszervezet (ESZ) egy szövegszerkesztő programban vezeti a tagok listáját.

- ↪ A táblázat tartalmazza a tag nevét, email címét, és a befizetett tagdíj mértékét.
- ↪ A szakszervezet munkatársa a táblázat szerkesztése közben az intranet helyett a nyilvános honlapra töltötte fel a dokumentumot.
- ↪ A neten, ha valaki rákeresett a szakszervezetre, akkor a táblázatot a keresőoldal is kilistázta és a fájlt bárki megnyithatta.
- ↪ A hiba egy jószándékú bejelentésen keresztül került nyilvánosságra.
- ↪ A dokumentumot 56-szor töltötték le mielőtt a törlésre került volna a nyilvános elérés.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	IGEN	IGEN
		



Példa (5)

Az Egyik Klinika főnövére egy excel táblázatban vezetteti a nővérképzőbe járó tanulók elérhetőségét mivel a Klinikán teljesítik gyakorlatukat.

- ✚ A Klinika adminisztratív munkatársa át szeretné alakítani a táblázatot, de véletlenül kitörli a tanulók e-mail címét tartalmazó oszlopot.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	NEM	NEM
		



Példa (6)

Áramszünet miatt leáll a szerver, így a rendszerben tárolt személyes adatok nem érhetők el kb. 15 percig.

➡ Ugyan az áramszünet alatt keletkezett egészségügyi adatokat pótlólag kell felvinni a rendszerbe, de adatsérülés nem következik be és a páciens ellátása sem szenvedett csorbát ezen rövid idő alatt.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
NEM	NEM	NEM
		



Példa (7)

Ellopnak egy számítógépet (laptopot) és egy adathordozót (pendrive), amin az orvosi rendszerben tárolt adatok egyik másolata van titkosított formában.

➡ A titkosítás, mint adatbiztonságot védő intézkedés miatt az adatokhoz nem fér hozzá a tolvaj.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	NEM	NEM
		

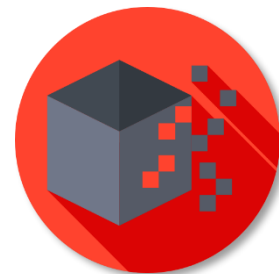


Példa (8)

Az orvos által használt IT rendszerhez illetéktelenek hozzáférnek.

➡ Így az ott tárolt valamennyi személyes adathoz is hozzáférhetnek.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	IGEN	IGEN
		



Példa (9)

Vírus-támadás éri a számítógépes hálózatot, a támadással nem kerültek illetéktelen személy birtokába páciensek adatai

➡ A támadás pillanatában bevitt adatokról nem készül biztonsági mentés, az adatok elvesznek.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	IGEN	IGEN
		



Példa (10)

Meghibásodás miatt elvesznek a betegnyilvántartásban tárolt adatok a szerverről.

➡ A biztonsági másolatból helyre lehet azokat állítani.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	NEM	NEM
		



Példa (11)

Az egészségügyi papíralapú kartonokat több nap után sem találják.

- ↪ Nem várt helyről, a szekrény mögé becsúsztatva, de néhány nap elteltével mégis csak előkerülnek.
- ↪ Sérelem nem éri a beteget.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	NEM	NEM
		



Példa (12)

Az orvos nem találja egyes betegei papíralapú kartonjait.

➡ Hosszas keresés után sem kerülnek elő.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	IGEN	IGEN
		

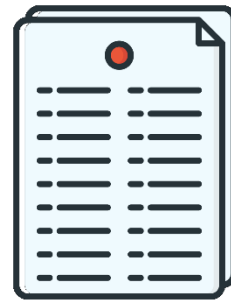


Példa (13)

A váróteremben kifüggesztésre kerül egy adott betegséggel kapcsolatban a kezelt betegek névlistája.

↪ Bárki által aki ott tartózkodik, szabadon elolvasható.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	IGEN	IGEN
		



Példa (14)

Az orvos további kezelés érdekében beutalót ír a betegének.

➤ A beutaló átadásakor azonban egy másik beteg leletét adja át.

➤ Csak utólag veszi észre otthon a beteg és jelzi ezt a kezelési helyen.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	IGEN	IGEN
		

Beküldő kódja: _____

Orvosi Beutalás - Javaslat
(szakrendelésre, gyógyászati segédeszközre, megjelenésről, stb.)


Név:
Anyja neve:
Lakcím:
Kor: TAJ sz.:

T:
Kérem szíves szakvizsgálatát.
Körleme: BNO:

PH: év hó n.

Köszönettel: orvos aláírása

*Az orvosi rendelésen való megjelenés igazolása táppénzre nem jogosít!
A. 3510-64/a. r.sz. - Kamikar Kft.

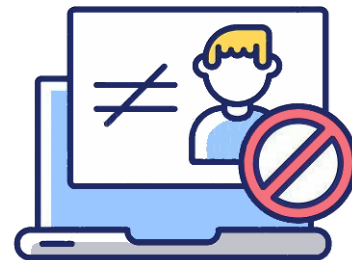


Példa (15)

Az asszisztens nem dolgozik tovább az orvossal kilép az egyetemről és más helyen dolgozik tovább.

- A betegnyilvántartó szoftverhez való hozzáférését nem szüntetik meg.
- Továbbra is hozzáfér a betegek adataihoz.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	IGEN	IGEN
		



Példa (16)

A beteg vérvételi eredményét rossz e-mail címre továbbítják.

➡ Így olyan személyhez jut el, aki ugyan akaratán kívül, de jogosulatlanul fér hozzá egészségügyi adatokhoz.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	IGEN	IGEN
		



Példa (17)

A számítógép meghibásodik.

- ➡ A beteg csak később jut hozzá a neki átadandó zárójelentéséhez.
- ➡ A központi rendszerben tárolt adatok nem sérültek.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
NEM	NEM	NEM
		



Példa (18)

Az adatkezelő által üzemeltetett weboldal időpontfoglaló rendszerében elérhető orvosi leletek és beutalók nyilvánosan hozzáférhetők és letölthetők olyan felhasználók részére is, akik nem rendelkeznek a megfelelő jogosultsággal.

- ↪ Egy bejelentő a feltárt biztonsági hibát eredménytelenül jelezte az adatkezelőnél.
- ↪ Az adatkezelő az adatvédelmi hiányosságot azután sem jelentette a Hatóságnak, miután a bejelentő azt a tudomására hozta.

Nyilván kell tartani	Hatóság (NAIH) értesítése	Érintett értesítése
IGEN	IGEN	IGEN
		



Forrás

- ❑ Árvay Viktor György - **Az adatvédelmi incidens – Nemzeti Közszerológati Egyetem**, Budapest, 2019
- ❑ Európai Bizottság honlapja, **Adatvédelem**, 2019
 - ➔ https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations_hu
- ❑ **Magyarázat a GDPR-ról**, Szerkesztő(k): Dr. Péterfalvi Attila, Dr. Révész Balázs, Dr. Buzás Péter, Wolters Kluwer Kiadó, Budapest 2018
- ❑ Szabó Endre Győző - **Adatvédelmi incidensek** - Adatvédelmi tisztviselők 2019. évi konferenciája - **NAIH DPO**
- ❑ **Adatvédelmi incidensek** - Adatvédelmi tisztviselők 2020. évi konferenciája - **NAIH DPO**



□ *Köszönöm a figyelmet !*

